ENHANCING OPERATIONAL SECURITY

Problem:
• Improving the effectiveness and efficiency of monitoring, analysis and reporting on information transmitted from unclassified communications sources throughout the AFNet enterprise, including phone, E-mail, RF, and Internet-Based Capabilities

Solution:
• Enhanced OPSEC disclosure effectiveness and accuracy
• Reduced risk of cyber security threats across the AFNET enterprise in support of US military battle plans, missions, and national security
• Increased compliance with DoD-wide directives and policies such as DISA's JRSS, NIST, and RMF

Customer Challenges

The USAF created a program specifically to provide real-time operational security (OPSEC) disclosure and cybersecurity risk assessment to Field Commanders, OPSEC Monitors, and other USAF and Joint forces personnel. Our customer needed innovative capabilities and technologies integrated into the program baseline to improve the effectiveness and efficiency of monitoring, analysis and reporting on information transmitted from unclassified communications sources throughout the AFNet enterprise, including phone, E-mail, RF, and Internet-Based Capabilities.

AI Solution Features

AI successfully implemented the first OPSEC, Data Loss Protection (DLP), Insider Threat, and PII oversight systems for the Air Force Special Operations Command (AFSOC), and the first cyber weapon system migration to DISA's Joint Regional Security Stacks (JRSS). Our security engineers helped implement a new insider threat call support technology for the 68th NWS weapon systems, enabling our engineers and cyber analysts to provide structured analysis of speech, and sifting for specific interactions and conversations to identify insider threat potential. For the USAF Cyberspace Defense Analysis Weapon System, AI's security engineers operate, maintain, and enhance the suite of

Fidelis XPS Sensors to identify and block insider threats and prevent data theft and unauthorized data transfer. We provide local system support at JBSA and at various CONUS and OCONUS locations.

Benefits to the Customer Mission

AI's cybersecurity engineers have provided innovative solutions to enhance the technical capabilities of our customer. We have enabled them to stay ahead of curve in terms of compliance with DoD policies and directives. Our support resulted in the following benefits:

- Enhanced OPSEC disclosure effectiveness and accuracy
- Reduced risk of cyber security threats across the AFNET enterprise in support of US military battle plans, missions, and national security
- Increased compliance with DoD-wide directives and policies such as DISA's JRSS, NIST, and RMF